Gauss's Lemma

JWR

November 20, 2000

Theorem (Gauss's Lemma). *Suppose that $f(x) \in \mathbb{Z}[x]$ has relatively prime coefficients, i.e.*

$$f(x) = c_n x^n + \cdots + c_1 x + c_0$$

where $(c_0, c_1, \in c_n) = 1$, i.e. $c_0, c_1, \ldots, c_n$ have no common factor. Assume that $f(x)$ is reducible in $\mathbb{Q}[x]$, i.e.

$$f(x) = A(x)B(x)$$

where $A(x), B(x) \in \mathbb{Q}(x)$ have positive degree. Then $f(x)$ reducible in $\mathbb{Z}[x]$; in fact,

$$f(x) = a(x)b(x)$$

where $a(x) = \mu A(x)$, $b(x) = \mu^{-1}B(x)$, $\mu \in \mathbb{Q}$, and $a(x), b(x) \in \mathbb{Z}[x]$.

Proof: Let m be a common multiple m of the denominators of the coefficients of $A(x)$ so $m_1 A(x) \in \mathbb{Z}[x]$. Let ℓ be the greatest common divisor of the coefficients of $m_1 A(x)$ so that $m_1 A(x) = \ell_1 a(x)$ where the coefficients of $a(x)$ are relatively prime. Similarly find nonzero integers integers m_1, ℓ_2 so $m_2 B(x) = \ell_2 b(x)$ where where the coefficients of $b(x)$ are relatively prime. Let $\mu = m_1/\ell_1$ and $\nu = m_2/\ell_2$. Then

$$f(x) = \mu\nu a(x)b(x)$$

where $a(x), b(x) \in \mathbb{Z}[x]$ are given by

$$a(x) = a_r x^r + \cdots + a_1 x + a_0, \qquad b(x) = b_s x^s + \cdots + b_1 x + b_0,$$

with $(a_0, a_1, \ldots, a_r) = (b_0, b_1, \ldots, b_s) = 1$ and $n = r + s$. By replacing $b(x)$ and ν by $-b(x)$ and $-\nu$ if necessary we may assume w.l.o.g. that $\mu\nu > 0$; We must show that $\mu\nu = 1$.

Write $\mu\nu = \ell/m$ where $m, \ell \in Z$, $m, \ell > 0$, and $(m, \ell) = 1$. Then

$$mf(x) = \ell a(x)b(x).$$

Now $\ell | mc_k$ for $k = 0, 1, \ldots n$ and $(m, \ell) = 1$ so $\ell | c_k$ for $k = 0, 1, \ldots n$. But $(c_0, c_1, \in c_n) = 1$ so $\ell = 1$. Assume that $m > 1$; we will derive a contradiction. Choose a prime p which divides m. Since $(a_0, a_1, \ldots, a_r) = 1$, p cannot divide all the coefficients in $a(x)$. Hence there must exist an integer i with $0 \leq i < r$

such that p divides each of $a_0, a_1, \ldots, a_{i-1}$ and p does not divide a_i. Similarly there must exist an integer j with and $0 \leq j < s$ such that p divides each of $b_0, b_1, \ldots, b_{j-1}$ and p does not divide b_j. But

$$mc_{i+j} = \cdots + a_{i-1}b_{j+1} + a_i b_j + a_{i+1}b_{j-1} + \cdots .$$

Now p divides the terms to the left of $a_i b_j$ (as $p|a_0$, $p|a_1$, $\ldots$, $p|a_{i-1}$), p divides the terms to the right of $a_i b_j$ (as $p|b_0$, $p|b_1$, $\ldots$, $p|b_{j-1}$), and p divides mc_{i+j} (as $p|m$). Thus $p|a_i b_j$ contradicting the fact that $p \not| a_i$ and $p \not| b_j$.

Eisenstein Criterion. *Suppose that $f(x) \in \mathbb{Z}[x]$ is given by*

$$f(x) = c_n x^n + \cdots + c_1 x + c_0$$

and p is a prime which satisfies

(1) *p does not divide c_n;*

(2) *p divides $c_{n-1}, \ldots, p_1, p_0$;*

(3) *p^2 does not divide c_0.*

Then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Proof: Suppose not, we will derive a contradiction. Because irreducibility in $\mathbb{Q}[x]$ is unaffected by dividing a nonzero element of $\mathbb{Z}$, we may assume w.l.o.g. that the coefficients $c_0, c_1, \ldots, c_n$ have no common prime factor. Then by Gauss's Lemma we have a factorization

$$f(x) = a(x)b(x)$$

where $a(x), b(x) \in \mathbb{Z}[x]$ and both factors have positive degree. Write

$$a(x) = a_r x^r + \cdots + a_1 x + a_0, \qquad b(x) = b_s x^s + \cdots + b_1 x + b_0.$$

By (2) $p|c_0$ so, as $c_0 = a_0 b_0$, either $p|a_0$ or $p|b_0$. W.l.o.g. assume the former. Then by (3) $p \not| b_0$. Now

$$c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0$$

so (by (2) and induction on k) $p|a_k$ for $k = 0, 1, \ldots r$. (In this step we used $r < n$.) But now p divides all the coefficients of $a(x)$ so p divides all the coefficients of $f(x)$ and this contradicts (1).